Journal of Pure and Applied Algebra 48 (1987) 9-22
North-Holland

IRREDUCIBILITY RESULTS FOR SEPARATED VARIABLES EQUATIONS

M. FRIED*

University of Florida, FL 32611, and University of California, Irvine, CA 92717, U.S.A.

Communicated by C.A. Weibel
Received 25 March 1985
Revised 10 February 1986

Rational functions with variables separated, $f_1(X_1)+f_2(X_2)+\cdots+f_l(X_l)=f(X)$, $\deg(f_i)>0$, $i=1,\ldots,l$, appear in many applications. In characteristic 0, when $l\geq 3$ the variety defined by $f(X)=0$ is irreducible (Main Theorem, Section 1).

In most applications, however, $l=2$. Even excluding trivial cases (e.g., $f_1=-f_2$), there are reducible curves with variables separated (Example 2.4). When f_1 and f_2 are polynomials, of respective degrees n and m, if f_1 is *indecomposable* the irreducibility result holds excluding finitely many n. The (2,3)-problem (Section 2) illustrates pure group theory formulations. In search of infinitely many n for which there are nontrivially reducible curves $f(X)=0$ with $\deg(f_1)=n$, a natural parameter k appears. No new examples arise from $k=1$ or 2 (Proposition 2.10).

Introduction

Let K be a field of 0 characteristic and let $f_1,\ldots,f_l\in K(x)$ be nonconstant rational functions. Write $f_i(x)$ as $h_{i1}(x)/h_{i2}(x)$, $(h_{i1}, h_{i2})=1$ and $h_{i1}, h_{i2}\in K[x]$. Our main theorem concerns the algebraic set $V(f_1(X_1)+\cdots+f_l(X_l))$ in affine l-space, A^l, defined by the equation

$$\left(\prod_{i=1}^{l} h_{i2}(X_i)\right)(f_1(X_1)+\cdots+f_l(X_l))=0. \tag{1}$$

Main Theorem. *If $l\geq 3$, then $V(\sum_{i=1}^{l} f_i)$ is irreducible.*

The case where $f_1,\ldots,f_l$ are polynomials appears in [16,19] in characteristic 0, and in [19] in positive characteristic. Also [15] considers the case that $f_1,\ldots,f_l$ are entire functions.

The proof (Section 1) works for arbitrary characteristic different from 2 if we add the hypothesis that there is no additive polynomial $m\in K[y]$, $\deg(m)>1$, such that

* Visiting Lady Davis Research professor, Hebrew University, Fall 1984.

$$f_i(x) - f_i(0) = m(\bar{f}_i(x)) \quad \text{for some } \bar{f}_i \in K(x),\ i = 1, \ldots, l, \tag{2}$$

and

$$m(y) + \sum_{i=1}^{l} f_i(0) \text{ is reducible over } K. \tag{3}$$

The main theorem responds affirmatively to a question of M. Jarden that was apparently presented to the author and A. Schinzel at roughly the same time. The proof in [18], even in the characteristic 0 case is quite long and it suggests no general principles. Our proof is based on the short and purely Galois theoretic [5, Proposition 2] (the basis of results of the author's discussed in [17]). Since this has applications to many problems, we have given here (Lemma 1.1) a generalized version of [5, Proposition 2]. In this conceptual framework the proof of the polynomial case of the main theorem follows an easy version of the expressions (12a), (13a) and the last paragraph of the proof of Part 4 of the Main Theorem.

Let $\boldsymbol{P}^1_x$ denote projective 1-space with an inhomogeneous uniformizing parameter x. The case $l=2$ in (1) amounts to looking at a fiber product $\boldsymbol{P}^1_{x_1} \times_{\boldsymbol{P}^1_y} \boldsymbol{P}^1_{x_2}$ given by $f_1 : \boldsymbol{P}^1_{x_1} \to \boldsymbol{P}^1_y$ and $-f_2 : \boldsymbol{P}^1_{x_2} \to \boldsymbol{P}^1_y$. Section 2 discusses the *(n, m)-problem: If f_1, f_2 are polynomials of respective degrees n and m which are suitably general, do there exist polynomials f_1', f_2' such that $V(f_1(f_1') + f_2(f_2'))$ is reducible*?

In order to exclude trivial situations of reducibility in the case $l=2$ we introduce the concept of newly reducible pairs (h, g) (Definition 2.1). Of necessity, newly reducible pairs of *polynomials* must be of the same degree (i.e., $\deg(h) = \deg(g)$ from Theorem 2.3). From the classification of finite simple groups [3,9] if (h, g) is newly reducible and h is not a composition of lower degree polynomials, then $\deg(h)$ must be 7,11,13,15,21 or 31. It is unknown, even, if there are infinitely many values of $\deg(h)$ for which (h, g) is newly reducible.

Application of Riemann's existence theorem to Lemma 1.1 translates the (n, m)-problem into pure group theory involving the integer parameter $k = \gcd(n \deg(f_1'), m \deg(f_2'))/\operatorname{lcm}(n, m)$ (Theorem 2.6). We note that the (2,2)-problem has a negative answer. Thus the (2,3)-problem is the first serious case (some discussion appeared in [14] which refers to the existence of Theorem 2.6 through private correspondence, and [1] related to connectedness of (1) for $l=2$). We show that neither $k=1$ nor 2 give solutions to the (2,3)-problem (Proposition 2.10).

On the one hand, affirmative solutions to the (n, m)-problem for all pairs (n, m) easily produces infinitely many values of $\deg(h)$ for which (h, g) is newly reducible. On the other, a negative solution even to the (2,3)-problem suggests a strange rarity of newly reducible polynomial pairs, and perhaps a simple classification of the polynomial pairs f_1, f_2 for which $V(f_1 + f_2)$ is reducible. Speculation here, however, should await results on $k = 3, 4, \ldots$ in the (2,3)-problem.

Connectivity results for fiber products far more general than those of this paper appear in [11,13]. These have application to the computation of fundamental groups of open subsets of projective space [13]. And irreducibility results, of necessity more special, have been applied to discussion of the action of the absolute Galois group of $\mathbb{Q}$ on various moduli spaces [6,8] (e.g., Jarden applies the Main

Theorem to the theory of real fields by concluding a trivial action for complex conjugation on the components of (1)).

Lemma 2.9 is due to W. Feit and L. Scott.

1. Proof of the Main Theorem

For V a variety defined over a field K, denote by $K(V)$ the field of rational functions on V. Let $\varphi: W \to V$ be a birational morphism of varieties defined over K. Assume that φ is generically finite so that φ induces a field extension $K(W)/K(V)$. Denote by $\overline{K(W)}$ the *normal closure* of this extension: $\overline{K(W)}$ is the smallest extension of $K(W)$ with the property that all isomorphisms of $\overline{K(W)}$ into field extensions of $K(V)$, that are fixed on $K(V)$, are automorphisms. The automorphism group, $\mathrm{Aut}(\overline{K(W)}/K(V))$ (or just $\mathrm{Aut}(\bar{W}/V)$), has a natural faithful permutation representation,

$$T(W/V) = T: \mathrm{Aut}(\bar{W}/V) \to S_n, \tag{4}$$

with $n = (\mathrm{Aut}(\bar{W}/V) : \mathrm{Aut}(\bar{W}/W))$ through the action of $\mathrm{Aut}(\bar{W}/V)$ on the left cosets of $\mathrm{Aut}(\bar{W}/W)$.

Given $\varphi_i: W_i \to V$, $i = 1, 2$, finite morphisms, counting the irreducible components of $W_1 \times_V W_2 = \{(w_1, w_2) \mid w_i \in W_i,\ i = 1, 2, \text{ and } \varphi_1(w_1) = \varphi_2(w_2)\}$ is a birational matter which our first lemma interprets entirely Galois theoretically. Denote the composite of $\overline{K(W_1)}$ and $\overline{K(W_2)}$ by $\overline{K(W_1, W_2)}$. Then $G = \mathrm{Aut}(\overline{K(W_1, W_2)}/K(V))$ is canonically identified with

$$\{(\sigma_1, \sigma_2) \in \mathrm{Aut}(\bar{W}_1/V) \times \mathrm{Aut}(\bar{W}_2/V) \mid \sigma_1|_L = \sigma_2|_L\} \tag{5}$$

where $L = \overline{K(W_1)} \cap \overline{K(W_2)}$. Furthermore, the fixed field, L^{f}, of G is the maximal inseparable extension of $K(V)$ in $\overline{K(W_1, W_2)}$. Finally, let $T_i: G \to S_{n_i}$ be the permutation representation of G associated to the subgroup $\mathrm{Aut}(\overline{K(W_1, W_2)}/K(W_i))$, $i = 1, 2$. Denote $\{\sigma \in G \mid T_i(\sigma)(1) = 1\}$ by $G(T_i)$, $i = 1, 2$, and denote $[\overline{K(W_1)} \cap \overline{K(W_2)} \cap L^{\mathrm{f}} : K(V)]$ by $m = m(W)$.

Lemma 1.1. *There is an $m(W)$-to-one association between irreducible components (counted with multiplicity) of $W_1 \times_V W_2$ and orbits of the group $G(T_1)$ under the permutation representation T_2.*

There exists a variety, W_i', that fits in a diagram of finite morphisms

$$W_i \to W_i' \xrightarrow{\varphi_i'} V, \quad i = 1, 2, \tag{6}$$

with the following properties: $\overline{K(W_1')} = \overline{K(W_2')}$; and the irreducible components of $W_1 \times_V W_2$ are in one-one correspondence with the irreducible components of $W_1' \times_V W_2'$.

Proof. Use the notation prior to the lemma. Let v be a generic point of V and let

$w_{i1}, \dots, w_{in_i}$ be the points of W_i that lie over υ, $i=1,2$. Identify $K(\upsilon)$, the field obtained by adjoining the coordinates of υ to K, with $K(V)$. Thus $K(\upsilon, w_{ij}, j=1,\dots,n_i, i=1,2)$ naturally is identified with $\overline{K(W_1, W_2)}$ and the action of G on $w_{i1}, \dots, w_{in_i}$ is naturally identified with T_i, $i=1,2$. Clearly the points $(w_{1k}, w_{2l}) \in W_1 \times_V W_2$, $k=1,\dots,n_1$, $l=1,\dots,n_2$ run over generic points of irreducible components of $W_1 \times_V W_2$. Furthermore, two of these points correspond to the same irreducible component if and only if they lie in the same orbit under the action of G. Since G is transitive on $\{w_{11}, \dots, w_{1n_1}\}$, the orbits of G on $\{(w_{1k}, w_{2l}): 1 \le k \le n_1, 1 \le l \le n_2\}$ are in one-one correspondence with the orbits of $G(T_1)$ on $\{w_{2l}: 1 \le l \le n_2\}$. This proves the first sentence of the lemma except for the observation that each irreducible component appears with multiplicity $m(W)$.

To find W_i' satisfying the conditions of (6), we need only work with the function field, $K(W_i')$, of W_i', $i=1,2$. That is, we seek a field L_i' between $K(V)$ and $K(W_i)$, $i=1,2$, with these properties: the normal closure $\overline{L_1'}$ of $L_1'/K(V)$ is equal to the normal closure $\overline{L_2'}$ of $L_2'/K(V)$; and the orbits of $\mathrm{Aut}(\overline{L_2'}/L_2')$ acting on the cosets of $\mathrm{Aut}(\overline{L_2'}/L_1')$ in $\mathrm{Aut}(\overline{L_2'}/K(V))$ are in one-one correspondence with the orbits of $G(T_1)$ under T_2.

If $\overline{K(W_1)} = \overline{K(W_2)}$ we are done. Otherwise, with no loss we may assume that $K(W_1) \not\subseteq \overline{K(W_2)}$. Let $M_1' = K(W_1) \cap \overline{K(W_2)}$. From the theorem of natural irrationalities

$$\mathrm{Aut}(\overline{K(W_2)}/M_1') = \mathrm{Aut}(K(W_1)\overline{K(W_2)}/K(W_1)). \tag{7}$$

Since each automorphism of $K(W_1)\overline{K(W_2)}/K(W_1)$ extends to an automorphism of $\overline{K(W_1, W_2)}$, the orbits of $\mathrm{Aut}(\overline{K(W_2)}/M_1')$ on the cosets of $\mathrm{Aut}(\overline{K(W_2)}/K(W_2))$ are in one-one correspondence with the orbits of $G(T_1)$ under the representation T_2.

Now let $\overline{M_1'}$ be the normal closure of $M_1'/K(V)$. If $K(W_2) \subseteq \overline{M_1'}$ we are done. Otherwise, replace $\overline{K(W_2)}$ by $\overline{M_1'}$ and $K(W_1)$ by $K(W_2)$ in the argument above. By an induction on $[K(W_1):K(V)][K(W_2):K(V)]$ we are done. □

Corollary 1.2, a special case of Lemma 1.1, is a slight generalization of [5, Proposition 2]. Let $V = \boldsymbol{P}_y^1$, $W_i = \boldsymbol{P}_{w_i}^1$, $i=1,2$, in Lemma 1.1. Thus $\varphi_i: \boldsymbol{P}_{w_i}^1 \to \boldsymbol{P}_y^1$ is given by a rational function $\varphi_i(w_i) = y$ in w_i, $i=1,2$. The fiber product $\boldsymbol{P}_{w_1}^1 \times_{\boldsymbol{P}_y^1} \boldsymbol{P}_{w_2}^1$ has $\varphi_1(X_1) - \varphi_2(X_2) = 0$ as an affine open subset. For $w_i' \in K(w_i)$ with $y \in K(w_i')$, denote the normal closure of $K(w_i')/K(y)$ by $\overline{K(w_i')}$, $i=1,2$.

Corollary 1.2. *In the notation above assume that φ_i is a nonconstant (thus finite) map, $i=1,2$. There exists $w_i' \in K(w_i)$ with $K(y) \subset K(w_i')$ with the following properties, $i=1,2$: $\overline{K(w_1')} = \overline{K(w_2')}$, and if $\varphi_i'(w_i') = y$, $i=1,2$, then the irreducible factors of $\varphi_1'(X_1) - \varphi_2'(X_2)$ (with the denominators cleared as in (1)) are in one-one correspondence with the irreducible factors of $\varphi_1(X_1) - \varphi_2(X_2)$.* □

Now we are set up to consider the proof of the Main Theorem. Assume that $l \ge 3$ in (1). Let $\varphi_1(X_1) = f_1(X_1)$ and $\varphi_2(X_2) = -(f_2(X_2) + f_3(X_3) + \cdots + f_l(X_l))$, a rational

function in X_2 with coefficients in $K(X_3, \ldots, X_l)$. Recall that if $g = m_1/m_2 \in K(x)$ with $(m_1, m_2) = 1$ and $m_1, m_2 \in K[x]$, then $\deg(g)$ is defined to be $\max_{i=1,2}(\deg(m_i))$.

Corollary 1.3. *Assume that $V(\sum_{i=1}^{l} f_i)$ has at least 2 irreducible components. Then there exists $g \in K(x)$ and $G_2 \in K(X_2, \ldots, X_l)$ with g of degree at least 2, such that*

$$g(G_2(X_2, \ldots, X_l)) = \varphi_2(X_2). \tag{8}$$

Proof. Apply Corollary 1.2 with the field $K' = K(X_3, \ldots, X_l)$ replacing K. From the assumptions there exist φ_1', φ_1'', g, $G_2 \in K'(x)$ such that $\varphi_1'(\varphi_1''(X_1)) = \varphi_1(X_1)$ and (8) holds. Let $w_i' \in K(w_i)$, $i = 1, 2$, as in Corollary 1.2, so that $\varphi_1'(w_1') = y$. Then $K'(y)$ and $\overline{K(w_1')}$ are linearly disjoint over $K(y)$. Thus there is a one-one correspondence between the fields between $K(y)$ and $\overline{K(w_1')}$ and the fields between $K'(y)$ and $\overline{K'(w_1')}$. Since $K'(w_2') \subsetneq \overline{K'(w_2')} = \overline{K'(w_1')}$, there exists $w_2^* \in \overline{K(w_1')}$ such that $\alpha(w_2^*) = w_2'$ with $\alpha \in K'(x)$ a degree 1 rational function. Thus with $(g \circ \alpha^{-1}) = g^*$ and $\alpha \circ G_2 = G_2^*$ replacing g and G_2, (8) still holds. As $g^*(w_2^*) = y$, it is clear that $g^* \in K(x)$. With g^* replacing g, this concludes the proof. □

Proof of the Main Theorem. From Corollary 1.3 it suffices to show that (8), with $g \in K(x)$ of degree at least 2, is impossible. We organize the proof into 5 parts. The first 3 build on degree computations under the assumption $\mathrm{char}(K) = 0$. The last two list the modifications respectively, for the cases $\mathrm{char}(K) > 2$ and $\mathrm{char}(K) = 2$.

Part 1. *Application of $\partial/\partial X_3$ to sides of* (8). From the chain rule

$$\frac{\mathrm{d}}{\mathrm{d}x}(g(x))\Big|_{x=G_2(X_2)} \frac{\partial}{\partial X_3}(G_2(X_2)) = \frac{\mathrm{d}}{\mathrm{d}X_3}(-f_3(X_3)). \tag{9}$$

Now consider both sides of (9) as functions of X_2 only, so that the right side is regarded as a constant. Thus

$$\deg_{X_2}\left(\frac{\mathrm{d}}{\mathrm{d}x}(g(x))\Big|_{x=G_2}\right) = \deg_{X_2}\left(\frac{\partial}{\partial X_3}(G_2(X_2))\right). \tag{10}$$

The left side of (10) is $\deg((\mathrm{d}/\mathrm{d}x)(g(x)))\deg_{X_2}(G_2(X_2))$ and, from the rules for taking the derivative of a quotient, the right side of (10) is *at most*

$$2\deg_{X_2}(G_2(X_2)). \tag{11}$$

By comparing (11) with the left side of (10), conclude that either

$$\deg\left(\frac{\mathrm{d}}{\mathrm{d}x}(g(x))\right) = 1, \tag{12a}$$

or

$$\deg\left(\frac{\mathrm{d}}{\mathrm{d}x}(g(x))\right) = 2. \tag{12b}$$

Part 2. *Deductions about g.* Write g as m_1/m_2 under the assumptions preceding

Corollary 1.3. Since $(m_2, (\mathrm{d}/\mathrm{d}x)(m_2))$ is the only possible common factor of the numerator and denominator of $(\mathrm{d}/\mathrm{d}x)(g)$,

$$\deg\left(\frac{\mathrm{d}}{\mathrm{d}x}(g)\right)=\max\left[\deg\left[\frac{m_2^2}{\left(m_2,\frac{\mathrm{d}}{\mathrm{d}x}(m_2)\right)}\right],\deg\left[\frac{m_2\frac{\mathrm{d}}{\mathrm{d}x}(m_1)-m_1\frac{\mathrm{d}}{\mathrm{d}x}(m_2)}{\left(m_2,\frac{\mathrm{d}}{\mathrm{d}x}(m_2)\right)}\right]\right]$$

The first term inside the right side implies that $\deg(m_2)\leq 1$ and either

$$g(x)\in K[x] \quad \text{with } \deg\left(\frac{\mathrm{d}}{\mathrm{d}x}(g)\right) \text{ equal to 1 or 2,} \tag{13a}$$

or

$$g(x)=(ax^2+bx+c)/(x+d) \quad \text{for some } a, b, c, d\in K. \tag{13b}$$

Part 3. (8) *combined with* (13) *gives a contradiction.* First consider the more involved case (13b). With a linear change of x and replacement of g by $a'g(x)+b'$ for some $a', b'\in K$, we may with no loss assume that $g(x)=x+1/x$. For notational simplicity, assume also that $l=3$ (say, by treating $X_4,\ldots,X_l$ as constants adjoined to K).

Write G_2 as $u_1(X_2, X_3)/u_2(X_2, X_3)$ with u_1 and u_2 relatively prime polynomials in $K[X_2, X_3]$. In the notation of the opening of the paper

$$u_1/u_2+u_2/u_1=-(h_{21}/h_{22})(X_2)-(h_{31}/h_{32})(X_3). \tag{14}$$

A comparison of the denominators of both sides of (14) gives $u_1u_2=g_2(X_2)g_3(X_3)$. Therefore $u_1/u_2=v_1(X_2)v_2(X_3)$ with $v_1, v_2\in K(x)$. Apply $(\partial/\partial X_2)(\partial/\partial X_3)$ to both sides of (14) to conclude

$$\frac{\mathrm{d}v_1}{\mathrm{d}X_2}\frac{\mathrm{d}v_2}{\mathrm{d}X_3}(1+(v_1v_2)^{-2})=0, \quad \text{or} \quad \frac{\mathrm{d}v_1}{\mathrm{d}X_2}\frac{\mathrm{d}v_2}{\mathrm{d}X_3}=0.$$

That is, u_1/u_2 involves only one of the variables X_2 or X_3, a contradiction to $l\geq 3$.

For case (13a), assume with no loss that K is algebraically closed. Then as with the reduction above, assume that g is without constant or linear term. As above, if $G_2=u_1(X_2, X_3)/u_2(X_2, X_3)$, then u_2 can be written as $v_1(X_2)v_2(X_3)$ with $v_1, v_2\in K[x]$. Now look at the numerator of (9) to see that u_1 involves only X_3. By symmetry u_1 is constant, and the technique of the previous paragraph concludes the results.

Part 4. $\mathrm{char}(K)>2$. These comments can shorten some of [18]. In this case we must add to the list of (12) the possibility that $(\mathrm{d}/\mathrm{d}x)(g(x))$ is actually a constant. If we assume that K is algebraically closed, and linearly change $g(x)$, then $g(x)=ax+(g_1(x))^p$ where $g_1(0)=0$ and $a=0$ or 1. Our goal is to induct on the degree of g to show that it is a composition of additive polynomials on the basis of (8). This easily reduces us to the case that $a=1$. Furthermore, this induction proceeds quite nicely if we know that G_2 has a variables separated form. The assumptions also give that

$$\frac{df_i}{dX_i} = \frac{\partial}{\partial X_i}(G_2), \quad i = 2, 3.$$

In the case that g_1 is a polynomial this is quite a lot of information for a combinatorial attack on (8). [18, pp. 10–13] eliminates the possibility that g is a rational function by using arguments from [10], and even with our extra information, this perhaps deserves some attention with an eye to simplification. Finally, if (12a) or (12b) hold, since $\text{char}(K) > 2$ we still conclude that $\deg(m_2) \leq 1$ (i.e., (13) holds), and no new complications arise.

Part 5. $\text{char}(K) = 2$. There is a new possibility over that given in Part 4: we may have $\deg(m_2) = 2$. [18] carefully lists the outcome of this. □

2. The (n, m)-problem

In this section the field K is $\mathbb{C}$. Now we consider the case $l = 2$ in the Main Theorem context at the beginning of the introduction: How do we describe the pairs (f_1, f_2) of rational functions over $\mathbb{C}$ such that $V(f_1(X_1) + f_2(X_2))$ is reducible? Our first discussion and theorem is a rephrasing of this problem entirely in terms of group theory.

Start with an ordered pair of positive integers (n, m). Let $\mathcal{R}(n, m)$ denote the ordered pairs of rational functions in $\mathbb{C}(x)$ of respective degrees n and m: $\{(h_1, h_2; g_1, g_2) \mid h_1, h_2, g_1, g_2 \in \mathbb{C}[x], \max(\deg(h_1), \deg(h_2)) = n, \max(\deg(g_1), \deg(g_2)) = m$ and h_1, h_2 (resp., g_1, g_2) relatively prime$\}$. So $(h_1, h_2; g_1, g_2)$ represents $(h_1/h_2, g_1/g_2) = (h, g) \in \mathcal{R}(n, m)$. In the earlier discussion we are replacing f_1 by h and $-f_2$ by g. Similarly, replace w_1 by x and w_2 by z in Corollary 1.2.

Suppose for $(h, g) \in \mathcal{R}(n, m)$ there exists $m \in \mathbb{C}(x)$ with $\deg(m) > 1$ and $h = m(\bar{h})$, $g = m(\bar{g})$ for some $\bar{h}, \bar{g} \in \mathbb{C}(x)$. Then $V(h - g)$ is easily seen to be reducible. We say that (h, g) is *composite* with m, and if no such m exists, then (h, g) is noncomposite. Denote the collection of noncomposite pairs by $\mathcal{R}(n, m)^{\text{nc}}$.

Basic problem. Describe $\{(h, g) \in \mathcal{R}(n, m)^{\text{nc}} \mid V(h - g) \text{ is reducible}\}$.

Suppose that $h = \bar{h}(\bar{\bar{h}})$, $g = \bar{g}(\bar{\bar{g}})$ and either $\deg(\bar{\bar{h}})$ or $\deg(\bar{\bar{g}}) > 1$, where $V(\bar{h} - \bar{g})$ is reducible. Then $V(h - g)$ is reducible. We say that $V(h - g)$ has *inherited reducibility*. It is more instructive (at times) to avoid this situation.

Definition 2.1. Call (h, g) *newly reducible* if $(h, g) \in \mathcal{R}(n, m)^{\text{nc}}$ and is reducible, but has not inherited reducibility.

We apply Corollary 1.2 (and Lemma 1.1) to put this in Galois theoretic terms. Denote by $T(h)$ and $T(g)$, respectively, the representations called T_1 and T_2 in Lemma 1.1. Denote $\text{Aut}(\overline{\mathbb{C}(x)}/\mathbb{C}(y))$ by $G(\overline{\mathbb{C}(x)}/\mathbb{C}(y))$.

tion T_2. Furthermore there is a group G_i' properly contained between $G(T_i)$ and G, $i=1,2$, and $G_1' \neq G_2'$. Just one group G fits this description: the dihedral group D_4 of degree 4. Regard this as a subgroup of S_4 (given by T_1). Then, with no loss, $G(T_1)=\langle(2\ 4)\rangle$, $G(T_2)=\langle(1\ 3)(2\ 4)\rangle$, $G_1'=\langle(1\ 3),(2\ 4)\rangle$ and $G_2'=\langle(1\ 2\ 3\ 4)\rangle$. Finally, let $\sigma=((1\ 3),(4\ 3)(2\ 1),(1\ 2\ 3\ 4)^{-1})=T_1(\sigma)$. Then $T_2(\sigma)$, given by the action on the cosets of $G(T_2)$ is (up to equivalence) $((4\ 3)(2\ 1),(2\ 4),(1\ 2\ 3\ 4)^{-1})$. Thus Theorem 2.3(a) holds. Since h' and g' are determined (up to linear change of variables) by the location of the branch points of $h': \boldsymbol{P}^1_{x'} \to \boldsymbol{P}^1_y$ and $g': \boldsymbol{P}^1_{z'} \to \boldsymbol{P}^1_y$, we obtain the hereditary reducibility of all degree 2 pairs (h', g') of polynomials by varying the finite branch points $y(1)$ and $y(2)$ of the covers with branch cycles given by σ (i.e., ∞ corresponds to the 4-cycle).

Thus the first serious case of the (n, m)-problem is the (2,3)-problem, and this is the case on which we concentrate for the remainder of the paper. As with the (2,2)-problem we can rephrase the (2,3)-problem entirely in terms of group theory.

Consider 6-tuples $(G, T_1, T_2, \sigma, \psi, k)$ with these properties: T_1 and T_2 are faithful inequivalent permutation representations of G, both of degree $6k$; $\psi: G \to S_2 \times S_3$ is a surjective homomorphism; $\sigma=(\sigma(1),\dots,\sigma(r))$, $G(\sigma)=G$ and $\sigma(1)\cdots\sigma(r)=1$; and if $\mathrm{pr}_1: S_2 \times S_3 \to S_2$, $\mathrm{pr}_2: S_2 \times S_3 \to S_3$ are the projections, then

$$(\mathrm{pr}_1 \circ \psi)(\sigma(r))=(1\ 2)=(\mathrm{pr}_1 \circ \psi)(\sigma(1)),$$
$$(\mathrm{pr}_1 \circ \psi)(\sigma(i))=1, \quad i=2,\dots,r-1, \tag{18a}$$

and

$$(\mathrm{pr}_2 \circ \psi)(\sigma(r))=(3\ 2\ 1), \qquad (\mathrm{pr}_2 \circ \psi)(\sigma(2))=(1\ 3),$$
$$(\mathrm{pr}_2 \circ \psi)(\sigma(3))=(1\ 2), \qquad (\mathrm{pr}_2 \circ \psi)(\sigma(i))=1, \quad i=1,4,5,\dots,r-1. \tag{18b}$$

In addition:

$$\sum_{j=1}^{r} \mathrm{ind}(T_i(\sigma(j)))=2(6k-1), \quad i=1,2; \tag{19a}$$

$T_1(\sigma(r))$ and $T_2(\sigma(r))$ are both $6k$-cycles; and (19b)

$G(T_1)$ is intransitive under T_2, but there is no length 1 orbit. (19c)

Theorem 2.6. *The* (2, 3)*-problem has an affirmative solution* (*equivalently, there exists hereditarily irreducible* $(h', g') \in \mathscr{P}(2,3)$) *if and only if there exists* $(G, T_1, T_2, \sigma, \psi, k)$ *satisfying* (18) *and* (19).

From Theorem 2.3 the selection of (h', g') only depends on the group theory of the branch cycles for the maps given by (h', g'). That means that the composite of the splitting fields of the field extensions defined by h' and g' must have a description of branch cycles that satisfies (18a) and (18b). Any representative pair of polynomials will suffice. Thus with no loss, in the (2,3)-problem, we could ask if

$(x^2, x(x-1)(x-2)) \in \mathscr{P}(2,3)$ is hereditarily irreducible. We will use k as a parameter by showing that $(G, T_1, T_2, \sigma, \psi, k)$ does not exist for $k=1$ or 2. That is, neither $k=1$ nor 2 works in the (2,3)-problem (note: $k=2$ *did* work in the (2,2)-problem). The next arguments, however, have general application.

Definition 2.7. Suppose that $f(y)=f_1(f_2(y))$ with $f_1, f_2 \in \mathbb{C}[y]$. Call this decomposition of f *in general position* if the images of the finite branch points of $f_2: \boldsymbol{P}^1_x \to \boldsymbol{P}^1_{x_1}$ under f_1 are all distinct and also disjoint from the finite branch points of $f_1: \boldsymbol{P}^1_{x_1} \to \boldsymbol{P}^1_y$.

Let $\overline{\mathbb{C}(x)}$ be the Galois closure $\mathbb{C}(x)/\mathbb{C}(y)$ with $f(x)=y$ as in Section 1 (similarly, for $\mathbb{C}(x_1)/\mathbb{C}(y)$ with $f_1(x_1)=y$ where $x_1=f_2(x)$). Denote by $\overline{\mathbb{C}(x|x_1)}$ the Galois closure of the extension $\mathbb{C}(x)/\mathbb{C}(x_1)$.

Lemma 2.8 (Fried [4, Lemma 15]). *Let $f=f_1(f_2)$ with $f_1, f_2 \in \mathbb{C}[x]$. Then there is an exact sequence*

$$1 \to H \to G(\overline{\mathbb{C}(x)}/\mathbb{C}(y)) \xrightarrow{\text{res}} G(\overline{\mathbb{C}(x_1)}/\mathbb{C}(y)) \to 1 \tag{20}$$

where H is isomorphic to a subgroup of $G(\overline{\mathbb{C}(x|x_1)}/\mathbb{C}(x_1))^{\deg(f_1)}$ that maps surjectively to $G(\overline{\mathbb{C}(x|x_1)}/\mathbb{C}(x_1))$ under projection onto each coordinate. In addition, if the decomposition of f is in general position, then H is isomorphic to $G(\overline{\mathbb{C}(x|x_1)}/\mathbb{C}(x_1))^{\deg(f_1)}$. □

As explained above, if k works in the (2,3)-problem, then there exist $h_1, g_1 \in \mathbb{C}[x]$ with $\deg(h_1)=3k$, $\deg(g_1)=2k$ and $V((h_1)^2-g_1(g_1-1)(g_1-2))$ is reducible.

Lemma 2.9 (W. Feit and L. Scott). *If h_1 and g_1 satisfy the properties above, then the decomposition of $(h_1)^2$ is not in general position (i.e., Definition 2.7 – either 0 is one of the branch points of $h_1: \boldsymbol{P}^1_z \to \boldsymbol{P}^1_x$ or one of the branch points is the negative of another).*

Proof. Go back to the formulation in expressions (18) and (19). From Lemma 2.8 the general position assumption implies

$$1 \to H_1 \times H_2 \to G \xrightarrow{\text{pr}_1 \circ \psi} S_2 \to 1 \tag{21}$$

is exact. Here $H_1=H_2(\cong G(\overline{\mathbb{C}(z|x)}/\mathbb{C}(x)))$ and conjugation by G interchanges $H_1 \times 1$ and $1 \times H_2$.

Let $M=\ker(\psi)$. Since S_3 has but one proper normal subgroup and $H_1 \times H_2 \xrightarrow{\text{pr}_2 \circ \psi} S_3$ is surjective, either $H_1 \times 1$ or $1 \times H_2$ maps surjectively to S_3 by $\text{pr}_2 \circ \psi$. Since $H_1 \times 1$ and $1 \times H_2$ are interchanged by conjugation, $H_1 \times 1/(H_1 \times 1) \cap M \simeq S_3$. But $M' = M/(H_1 \times 1 \cap M) \times (1 \times H_2 \cap M) \simeq S_3$ is a normal subgroup of $(H_1 \times 1/(H_1 \times 1 \cap M)) \times (1 \times H_2/(1 \times H_2 \cap M)) \simeq S_3 \times S_3$. To conclude the lemma check that there is no such

normal subgroup of $S_3 \times S_3$ stable under an automorphism interchanging the two factors. □

Proposition 2.10. *In the notation of Theorem* 2.6, *neither* $k=1$ *nor* 2 *works in the* (2, 3)*-problem.*

Proof. The case $k=1$, although not trivial, is immensely easier than the case $k=2$. Therefore we do only the latter. As in previous notation let $h=(h_1)^2$, $g=g_1(g_1-1)(g_1-2)$ with $\deg(h_1)=6$, $\deg(g_1)=4$ and $(h,g)\in\mathscr{P}(12,12)$ newly reducible. This use of actual polynomials will be a mnemonic aid for following these truly group theoretic arguments while still incorporating the Riemann–Hurwitz conditions (19). Define x and z by $h(x)=y$ and $g(z)=y$. Also let $h_1(x)=x_1$ and $g_1(z)=z_1$ (i.e., $x_1^2=y$). From Lemma 2.2, $\overline{\mathbb{C}(x)}=\overline{\mathbb{C}(z)}$ and we denote $G(\overline{\mathbb{C}(x)}/\mathbb{C}(y))$ by G.

Call $m\in\mathbb{C}[w]$ a *cyclic* (resp., *Chebychev*) polynomial if, with $m(w)=y$, $G(\overline{\mathbb{C}(w)}/\mathbb{C}(y))$ is cyclic (resp., the dihedral group of degree $\deg(m)$). If m is indecomposable and neither cyclic nor Chebychev, then, in the notation prior to Lemma 2.3,

$$T(h) \text{ is doubly transitive [4, Theorem 1].} \tag{22}$$

Let H_h (resp., H_g be the kernel of $\mathrm{res}: G(\overline{\mathbb{C}(x)}/\mathbb{C}(y))\to S_2$ (resp., $\mathrm{res}: G(\overline{\mathbb{C}(z)}/\mathbb{C}(y))\to S_3$). Since $\overline{\mathbb{C}(x)}=\overline{\mathbb{C}(z)}$, $|H_h|=3\,|H_g|$. From Lemma 2.8, $|G(\overline{\mathbb{C}(x|x_1)}/\mathbb{C}(x_1))|$ (resp. $|G(\overline{\mathbb{C}(z|z_1)}/\mathbb{C}(z_1))|$) divides $|H_h|$ (resp., $|H_g|$) which in turn is a *proper* divisor of $|G(\overline{\mathbb{C}(x|x_1)}/\mathbb{C}(x_1))|^2$ (resp., a divisor of $|G(\overline{\mathbb{C}(z|z_1)}/\mathbb{C}(z_1))|^3$. If h_1 is indecomposable, then (22) implies that $G(\overline{\mathbb{C}(x|x_1)}/\mathbb{C}(x_1))$ is doubly transitive. Thus $|H_h|$ is divisible by 5. But, $G(\overline{\mathbb{C}(z|z_1)}/\mathbb{C}(z_1))\subseteq S_4$, and $5\nmid|H_g|$ – a contradiction. Thus $h_1=\bar{h}_1(\bar{h}_2)$. Divide into two cases.

Case 1. $\deg(\bar{h}_1)=2$, $\deg(\bar{h}_2)=3$. Decompose h as $h_1'(h_2')$ with $h_1'=(\bar{h}_1)^2$, $h_2'=\bar{h}_2$. Easily exclude the possibility that h_1' is a cyclic polynomial. From Lemma 2.8 there is an exact sequence $1\to H'\to G\to G(\overline{\mathbb{C}(\bar{x}_1)}/\mathbb{C}(y))\to 1$ with $\bar{x}_1=\bar{h}_2(x)$ and H' a subgroup of $(S_3)^4$. Since (h,g) is newly reducible $G_1=G(T(g))$ is a subgroup of G of index 12, intransitive under $T(h)$, with $\mathrm{res}(G_1)$ (restriction to $\overline{\mathbb{C}(\bar{x}_1)}$) transitive in the representation given by the cosets of $G(\overline{\mathbb{C}(\bar{x}_1)}/\mathbb{C}(\bar{x}_1))$. Also

$$(G:G_1)=12=(H':H'\cap G_1)(G(\overline{\mathbb{C}(\bar{x}_1)}/\mathbb{C}(y)):\mathrm{res}(G_1)).$$

As the subgroup of S_3 of order 3 is transitive, note that G_1 is transitive if 3 divides $|H'\cap G_1|$. Conclude that only one power of 3 divides H'. Clearly h_1' is a Chebychev polynomial: $|G(\overline{\mathbb{C}(\bar{x}_1)}/\mathbb{C}(y))|=8$. Therefore $|H_g|$ is a power of 2 and g_1 is also a Chebychev polynomial. Conclude from the following argument applied to g, contrary to the above, that $\mathrm{res}(G_1)$ is intransitive.

If m_1 is a Chebychev polynomial of degree 3 and m_2 is a Chebychev polynomial of degree 4, consider $m=m_1(m_2)$ and the exact sequence $1\to H_m\to G(\overline{\mathbb{C}(w)}/\mathbb{C}(y))\xrightarrow{\mathrm{res}} G(\overline{\mathbb{C}(w_1)}/\mathbb{C}(y))\to 1$, with $m(w)=y$, $m_2(w)=w_1$. Suppose H_1 is a subgroup of $G(\overline{\mathbb{C}(w)}/\mathbb{C}(y))$ of index 12. Since $|H_m|$ is a power of 2 and $G(\overline{\mathbb{C}(w_1)}/\mathbb{C}(y))=S_3$, conclude that $(G(\overline{\mathbb{C}(w_1)}/\mathbb{C}(y)):\mathrm{res}(H_1))$ is divisible by 3, so that $\mathrm{res}(H_1)$ is intransitive.

Case 2. $\deg(\bar{h}_1)=3$, $\deg(\bar{h}_2)=2$. Apply the argument of Case 1 to get an exact sequence $1\to H'\to G\to G(\overline{\mathbb{C}(\bar{x}_1)}/\mathbb{C}(y))\to 1$. Analogous to Case 1, G_1 is transitive if 2 divides $|H'\cap G_1|$ (and H' is a power of 2). Thus, from the formula for $(G:G_1)=12$ in terms of $(H':H'\cap G_1)$, we have $|H'|=2$ or 4, and $|G|$ divides $2\cdot(6)^2\cdot 4$.

If g_1 is not a Chebychev polynomial, then H_g has S_4 as a quotient (Lemma 2.8). Thus $|G|$ has $4\cdot 3\cdot 2\cdot 3\cdot 2=6^2\cdot 4$ as a divisor of its order (and $|G|$ divides $6^2\cdot 8$). The final argument of the proof will exclude this case, so that g is a composition of Chebychev polynomials and we conclude by the last paragraph of Case 1.

Suppose now that g_1 is not a Chebychev polynomial. Consider $u(z_1)=z_1(z_1-1)(z_1-2)$ as a map on the 3 finite branch points $z_1(1)$, $z_1(2)$, $z_1(3)$ of $g_1: \boldsymbol{P}^1_z\to \boldsymbol{P}^1_{z_1}$. If $u(z_1(1))$ is distinct from the branch points of the map given by u, and also from $u(z_1(j))$, $j=2,3$, it is easy to conclude, for f replaced by $g=u(g_1)$ in Lemma 2.8, that $|H|=(12)^3$. This contradicts the observation, above, that $|G|$ divides $6^2\cdot 8$.

Lemma 2.9 implies that $h=(\bar{h}_1(\bar{h}_2))^2$ has 3 (and not 4) finite branch points. This leaves only 2 possibilities up to reordering of branch points:

$$u(z_1(1))=u(z_1(2))=u(z_1(3)), \tag{23a}$$

or

$$u(z_1(1)) \text{ is one of the branch points of } u \text{ and } u(z_1(2))=u(z_1(3)). \tag{23b}$$

We write out typical branch cycle generators for the image of G in S_{12} under $T(g)$, where $\sigma(1)$ corresponds to $u(z_1(2))$ in each case, $\sigma(2)$ and $\sigma(3)$ correspond to the finite branch points of u and $\sigma(4)=(1\ 2\cdots 12)^{-1}$ corresponds to ∞. In this case the action of G on the sets $X_1=\{1,4,7,10\}$, $X_2=\{2,5,8,11\}$ and $X_3=\{3,6,9,12\}$ gives the map $\text{res}: G\to S_3$.

A typical case for branch cycles in case (23a) is given by

$$\sigma(1)=(2\ 5)(6\ 9)(1\ 10), \qquad \sigma(2)=(4\ 3)(1\ 9)(7\ 6)(10\ 12),$$
$$\sigma(3)=(1\ 5)(2\ 4)(7\ 8)(10\ 11). \tag{24}$$

From the above, the order of H_g cannot exceed $8\cdot 6$ (i.e., the kernel of projection of H_g on any factor of $(S_4)^3$ has order at most 2). But H_g contains $\sigma(1)$, $\sigma(4)^3$, and $\sigma(j)\sigma(1)\sigma(j)^{-1}$, $j=2,3,4$. Thus H_g contains $\sigma(2)\sigma(1)\sigma(2)\sigma(1)=(1\ 7)(9\ 12)(6\ 9)(1\ 10)=(1\ 10\ 7)(6\ 12\ 9)$: the kernel of the projection of H_g on the 1st factor of $(S_4)^3$ has order at least 3. This concludes the exclusion of (23a).

A typical case for branch cycles in case (23b) is given by the form

$$\sigma(1)=(2)(2), \qquad \sigma(2)=(2)(2)(4), \qquad \sigma(3)=(2)(2)(2)(2), \tag{25}$$

where $\sigma(1)$ leaves the sets X_1, X_2, X_3 fixed. In this case it is obvious that the kernel of the projection of H_g on the 1st factor of $(S_4)^3$ has order exceeding 2. □

Although long, the proof of Proposition 2.10 is based on clear algorithmic principles involving permutation groups with many systems of imprimitivity; a sharp

contrast to the technique that gave the results for newly reducible (h, g) with h indecomposable (as following Example 2.4). Alas, it may require the skills of a real group theorist to turn the ideas of Proposition 2.10 into a complete solution of the (n, m)-problem.

References

[1] S. Abhyancher and L. Rubel, Every difference polynomial has a connected zero-set, J. Indian Math. Soc. 43 (1979) 69–78.
[2] H. Farkas and M. Fried, The $g-1$-support cover of the canonical locus, J. Analyse Math. 46 (1986) 148–157.
[3] W. Feit, Some consequences of the classification of finite simple groups, Santa Cruz Conference on Finite Groups, Proc. Sympos. Pure Math. 37 (1980) 175–181.
[4] M. Fried, On a conjecture of Schur, Michigan Math. J. 17 (1970) 41–55.
[5] M. Fried, The field of definition of function fields and a problem in the reducibility of polynomials in two variables, Illinois J. Math. 17 (1973) 128–145.
[6] M. Fried, Fields of definition of function fields and Hurwitz families..., Comm. Algebra 5 (1) (1977) 17–82.
[7] M. Fried, Exposition on an arithmetic-group theoretic connection via Riemann's existence theorem, Santa Cruz Conference on Finite Groups, Proc. Sympos. Pure Math. 37 (1980) 571–602.
[8] M. Fried, On reduction of the inverse Galois group problem to simple groups, Proc. Rutgers Group theory year, 1983–84 (Cambridge University Press, Cambridge, 1985) 289–301.
[9] M. Fried, Rigidity and applications of the classification of finite simple groups to monodromy, Part II, Preprint.
[10] M. Fried and R.E. MacRae, On curves with separated variables, Math. Ann. 180 (1969) 220–226.
[11] W. Fulton and J. Hansen, A connectedness theorem for projective varieties, with applications to intersections and singularities of mappings, Ann. of Math. 110 (1979) 159–166.
[12] W. Fulton and R. Lazarsfeld, On the connectedness of degeneracy loci and special divisors, Acta Math. 146 (1981) 271–283.
[13] W. Fulton and R. Lazarsfeld, Connectivity and its applications in algebraic geometry, Preprint.
[14] L.A. Rubel, A. Schinzel and H. Tverberg, On difference polynomials and hereditarily irreducible polynomials, J. Number Theory 12 (1980) 230–235.
[15] L.A. Rubel, W.A. Squires and B.T. Taylor, Irreducibility of certain entire functions with applications to harmonic analysis, Ann. of Math. 108 (1978) 553–567.
[16] A. Schinzel, Some unsolved problems on polynomials in the book "Neki herešeni problem u matematici", Matematička Biblioteka Beograd 25 (1963) 63–70.
[17] A. Schinzel, Reducibility of polynomials, Actes Intern. Cong. Math. 1970, Vol. 1 (Gauthier-Villars, Paris, 1971) 491–496.
[18] A. Schinzel, Reducibility of polynomials in several variables II, Pac. J. Math. 118 (1985) 531–563.
[19] H. Tverberg, A remark on Ehrenfeucht's criterion for irreducibility of polynomials, Prace Mat. 8 (1964) 117–118.
[20] H. Tverberg, On the irreducibility of polynomials $f(x)+g(y)+h(z)$, Quart. J. Math. Oxford Ser. (2) 17 (1966) 364–366.